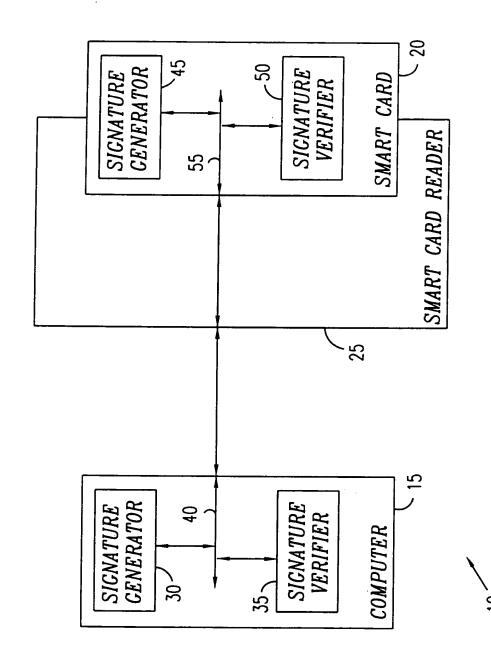
FIG. 1



A GENERATOR OF A PUBLIC-KEY SUPPLIES A SET FIG. 2A S1 OF k POLYNOMIAL FUNCTIONS AS A PUBLIC-KEY. WHERE THE SET STINCLUDES THE FUNCTIONS $P_1(x_1,...,x_{n+v}, y_1,...,y_k),..., P_k(x_1,...,x_{n+v}, y_1,...,y_k), WITH$ k, v, AND n BEING INTEGERS, $x_1,...,x_{n+v}$ BEING n+vVARIABLES OF A FIRST TYPE, AND $y_1, ..., y_k$ BEING k VARIABLES OF A SECOND TYPE, AND THE SET SI BEING OBTAINED BY APPLYING A SECRET KEY OPERATION ON A SET S2 OF k POLYNOMIAL **FUNCTIONS** $P'_{1}(a_{1},...,a_{n+v},y_{1},...,y_{k}),...,P'_{k}(a_{1},...,a_{n+v},y_{1},...,y_{k})$ WITH a₁,...,a_{n+v} BEING n+v VARIABLES WHICH INCLUDE A SET OF n "OIL" VARIABLES a₁,...,a_n, AND A SET OF v "VINEGAR" VARIABLES $a_{n+1},...,a_{n+v}$ 100 A MESSAGE TO BE SIGNED IS PROVIDED 105 A SIGNER OF A DIGITAL SIGNATURE APPLIES A HASH FUNCTION ON THE MESSAGE TO PRODUCE A SERIES OF k VALUES b₁,...,b_k 110 THE SIGNER SUBSTITUTES THE SERIES OF k 115 VALUES b_1, \dots, b_k FOR THE VARIABLES y_1, \dots, y_k OF THE SET S2 RESPECTIVELY SO AS TO PRODUCE A SET S3 OF k POLYNOMIAL FUNCTIONS $P''_{1}(a_{1},...,a_{n+v}),...,P''_{k}(a_{1},...,a_{n+v})$ 120 THE SIGNER SELECTS v VALUES a'n+1,...,a'n+v FOR THE v "VINEGAR" VARIABLES $a_{n+1},...,a_{n+v}$ 125 THE SIGNER SOLVES A SET OF EQUATIONS $P''_{1}(a_{1},...,a_{n},a'_{n+1},...,a'_{n+v})=0,...,P''_{k}(a_{1},...,a_{n},a'_{n+1},...,a'_{n+v})=0$ TO OBTAIN A SOLUTION FOR a'1,...,a'n 130 THE SIGNER APPLIES THE SECRET KEY

OPERATION TO TRANSFORM a'1,...,a'n+v TO

THE DIGITAL SIGNATURE $e_1,...,e_{n+v}$

FIG. 2B

200

A VERIFIER OF A DIGITAL SIGNATURE OBTAINS THE SIGNATURE $e_1,...,e_{n+\nu}$, THE MESSAGE, THE HASH FUNCTION AND THE PUBLIC KEY

205

THE VERIFIER APPLIES THE HASH FUNCTION ON THE MESSAGE TO PRODUCE THE SERIES OF k VALUES b_1,\ldots,b_k

210

The VERIFIER VERIFIES THE DIGITAL SIGNATURE BY VERIFYING THAT THE EQUATIONS

 $P_1(e_1,...,e_{n+v},b_1,...,b_k)=0,..., P_k(e_1,...,e_{n+v},b_1,...,b_k)=0$ ARE SATISFIED